The first step towards HIPAA compliance

What the HIPAA Security Rule entails and how to follow it

Abyde™

Components of HIPAA compliance

The Health Insurance Portability and Accountability Act, better known as HIPAA, contains the regulations required for healthcare providers as well as their business associates to ensure the security of protected health information (PHI) of any kind.

Within overall HIPAA law there are a series of rules outlining the necessary requirements of compliance. These rules each play a major role in assessing, documenting, and ultimately protecting the practice as well as their patients from the many risks associated with PHI data breaches.

So where do we start?

The first step in HIPAA compliance is defined within the Security Rule. The Security Rule essentially ensures that PHI will only be accessible to those who *should* have access. It is up to the practice to decide upon and implement the specific security safeguards needed to protect their practices' PHI. When deciding which security measures are necessary for your practice you should take into account:

- Practice size
- Capabilities
- Costs of specific security measures
- Operational impact

Seem like a lot? Don't worry we'll walk you through it.

DID YOU KNOW??

94% of covered entities audited by the **Office for Civil Rights** could not show a properly documented HIPAA risk management program.

**OCR, 2019*

The Security Rule

As we mentioned, the true purpose behind HIPAA compliance is to ensure the protection and confidential handling of PHI. The Security Rule sets the standard for all of the necessary safeguards a practice must have in place to protect the privacy of PHI.

What exactly do we mean by safeguards?

The Security Rule breaks down the three types of safeguards necessary to secure PHI from both intentional and unintentional use or disclosure that might be in violation of HIPAA.

1. Administrative Safeguards

The documented actions taken to select, implement, and maintain security measures to protect sensitive health information including managing the conduct of the practice's workforce.

2. Physical Safeguards

The documented measures to protect a practice's information systems and physical buildings and equipment from natural hazards as well as unauthorized intrusion.

3. Technical Safeguards

The documented strategies and solutions that practices implement to secure electronic protected health information and control access to it.

Administrative Safeguards

The first step of any solution is determining what exactly needs to be fixed. Within the provisions of the administrative safeguards, covered entities as well as their business associates are required to perform a security risk analysis specific to their organization.

What is a security risk analysis?

A complete risk analysis involves assessing and documenting what your organization is currently doing as well as addressing any areas necessary, and repeating this process on an ongoing basis. To properly analyze your processes, you should:

- ✓ Evaluate how likely and how great the impact would be of a data or physical breach
- ✓ Use these findings to implement the proper security measures to address these risks
- ✓ Document these chosen security policies including the reasons why these protections are necessary
- ✓ Continue to update and maintain these security measures over time

Other aspects of adhering to the proper Administrative Safeguards Include:

- Proper training of each employee on HIPAA compliance
- Designating a HIPAA Compliance Officer for your practice to implement these policies
- Completing Business Associate Agreements with all qualifying business vendors

83% of covered entities audited by the Office for Civil Rights **did not have a documented, comprehensive Security Risk Analysis**.

**OCR*

Physical Safeguards

Once you've determined your risks and documented the policies required to keep PHI secure, you must establish safeguards to protect the security of both the physical structure and the electronic equipment within your practice. You may already be implementing some of the more straightforward safeguards such as having locks on your practice doors as well as having alarms and other security systems installed.

Unauthorized Access/Improper Disclosure =

3 million+ patient records EXPOSED in 2018 alone.

What else is needed?

Besides the basic ways of protecting your practice's physical security, some of the things you'll also need to do include:

Provide clear and specific procedures for physical access to your practice.

Regulate who has direct access to the areas where PHI is located.

Ensure access is only made available to those that have had proper training.

Properly document your practice's policies to provide a guideline for the safeguards needed.

Additional steps such as controlling mobile device access and keeping a log of all hardware devices that house or transmit PHI.

And more!

Technical Safeguards

Protecting the technology that houses electronic PHI is a little more difficult than putting locks on the doors. Your practice should:

- Put technical policies in place which allow only authorized access to ePHI
- Implement special software or hardware to protect ePHI
- Ensure you have the ablity to trace system activity to a specific user
- Document and adhere to policies and procedures that ensure PHI will not be altered or disposed of improperly

When does data need to be safeguarded?

- ✓ Anytime it is accessed as well as when being sent or recieved from other practices.
- ✓ If it has any traceable identificaton that can be linked to a patient it must be encrypted prior to sending or recieving.

What exactly does encrypting data entail?

Encrypting data basically means making PHI unreadable to anyone other than the person sending the data and the person receiving it.

Properly encrypted PHI and firewalls are just one piece of ensuring your technology is safeguarded. Employees must be properly trained on appropriate access and these safeguards must evolve with the ever changing technological environment.

67% of Healthcare leaders think their organization will experience a cybersecurity attack this year.

*2018 Ponemon and Opes Survey

Now What?

In order to comply with the Security Rule, your practice should follow these basic steps:

1. Assess current security, risks, & gaps
2. Develop an implementation plan
3. Implement solutions
4. Document decisions
5. Reassess periodically

So how can you guarantee you are HIPAA compliant?

This is where a software solution like Abyde can be the best option for simplifying HIPAA compliance. Specific to the Security Rule requirements, Abyde offers everything your practice needs to guarantee compliance such as:

- An automated risk analysis that guides your practice through required assessment areas.
- Dynamically generated policies and procedures specific to your practice's workflows.
- Training videos as well as certificates of completion to ensure each employee within your practice is fully educated on HIPAA.

Following the requirements within the Security Rule is a vital first step towards ensuring your practice is HIPAA compliant, and we are here to help.

HIPAA SIMPLIFIED

Our goal at Abyde is to simplify a convoluted and complicated HIPAA compliance program and make HIPAA not only easy, but stress-free. Join a free educational webinar to learn how Abyde can help educate and automate your practice when it comes to stress-free HIPAA compliance. Register at abyde.com/webinar today!

RESPONSIVE AND INTUITIVE

CUSTOMIZED POLICY GENERATION

DITCH PAPER AND GAIN EASY ACCESS

MEET MACRA/MIPS REQUIREMENTS

AUDIT PROTECTION PROGRAM

Abyde™

Visit abyde.com/webinar for a free educational session on HIPAA compliance, or contact us at info@abyde.com to speak to a HIPAA expert.